Safety-Critical Systems

Prof. Chris Johnson

School of Computing Science, University of Glasgow.

johnson@dcs.gla.ac.uk

http://www.dcs.gla.ac.uk/~johnson

University of Glasgow

Terminology and the Ariane V Mishap

Prof. Chris Johnson,

School of Computing Science, University of Glasgow.

johnson@dcs.gla.ac.uk

http://www.dcs.gla.ac.uk/~johnson

PCMMU
LEFT AUDIO
LEFT COMM POWER
GPC STATUS
FAILED GPC
CRYO
O2 HTR ASSY TEMP
PRESS
QTY
H2
CABIN PRESS
SENSOR A
O1
O2
ASCENT TRAJ
EVENT TIME
39:50
MAIN ENGINE STATUS
WINDOW JETTISON HANDLE PIN
REMOVE BEFORE JETTISON

Terminology and the Arian 5 Case Study

- Introduction.
- Terminology.
- Accidents.
- Ariane 5 Case Study.

Overview

- Open assessment.
  - 30% on a practical exercise.
- Closed assessment.
- Nancy Leveson's, Safeware: System safety and computers, Addison-Wesley, ISBN 0-201-11972-2.
- http://www.dcs.gla.ac.uk/~johnson/book

Terminology

- What is `Safety‘?
- Nothing bad will happen?
  - Is this sufficient?
- System will not endanger human life or the environment (Storey, p.2).
- Freedom from accidents or losses (Leveson, p.181)

Terminology

- What is `Safety'?
- An absolute or relative term?
- Does it form a continuum?
- Can we ever be `absolutely' SAFE?

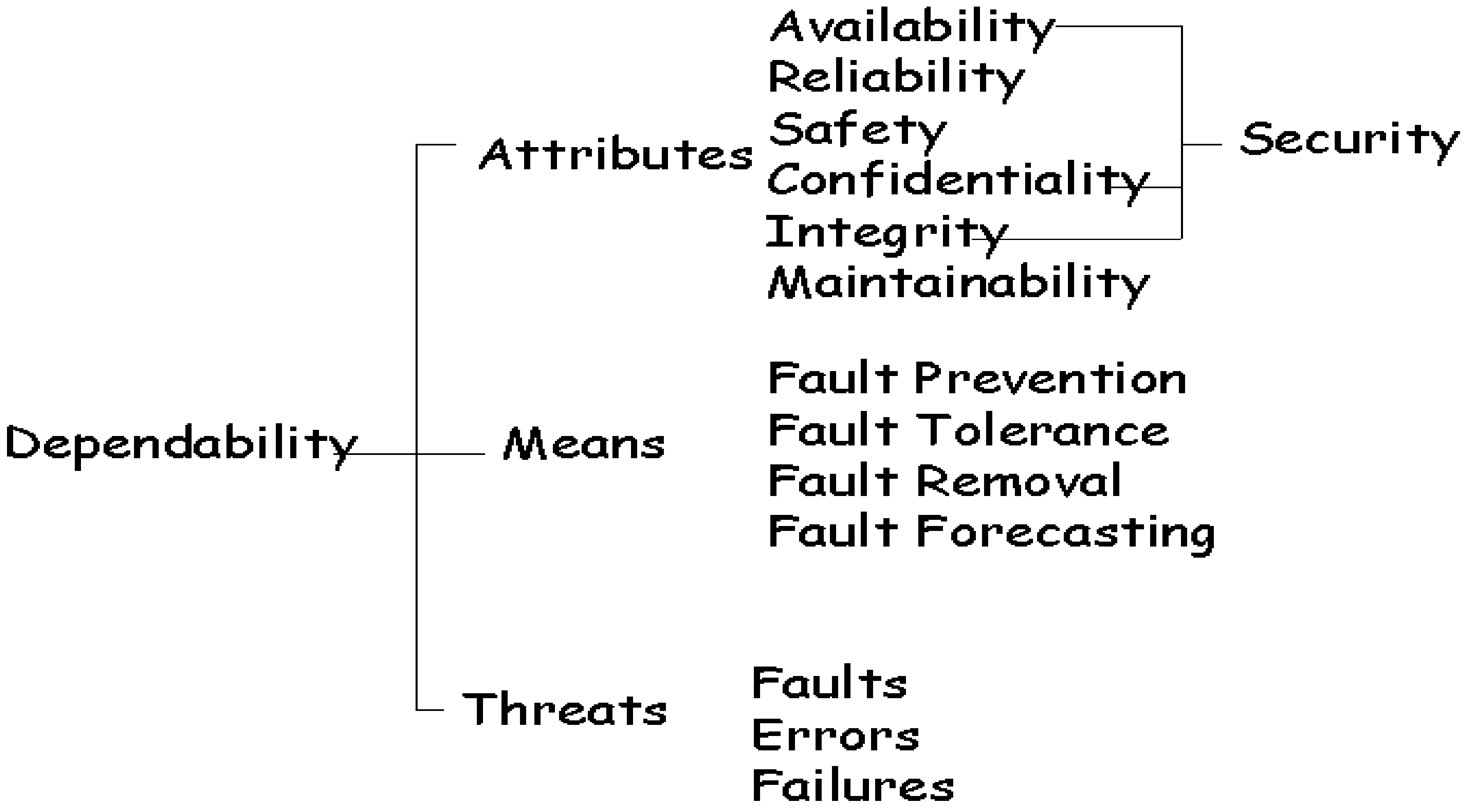
Terminology

- Is `Safety' Relative?
- Depends on individual view of risk.
- Risk = frequency x cost.
  - But cost or utility is subjective...
- Psychometric Risk Assessments.
- Biases, risk equity, target levels of risk…

Terminology

- What is `Safety'?
- Part of wider dependability?
- Ability to deliver a trusted service.
- J.C. Laprie's Diversity for Dependability

Terminology



- Dependability
  - Attributes
    - Availability
    - Reliability
    - Safety
    - Confidentiality
    - Integrity
    - Maintainability
  - Means
    - Fault Prevention
    - Fault Tolerance
    - Fault Removal
    - Fault Forecasting
  - Threats
    - Faults
    - Errors
    - Failures

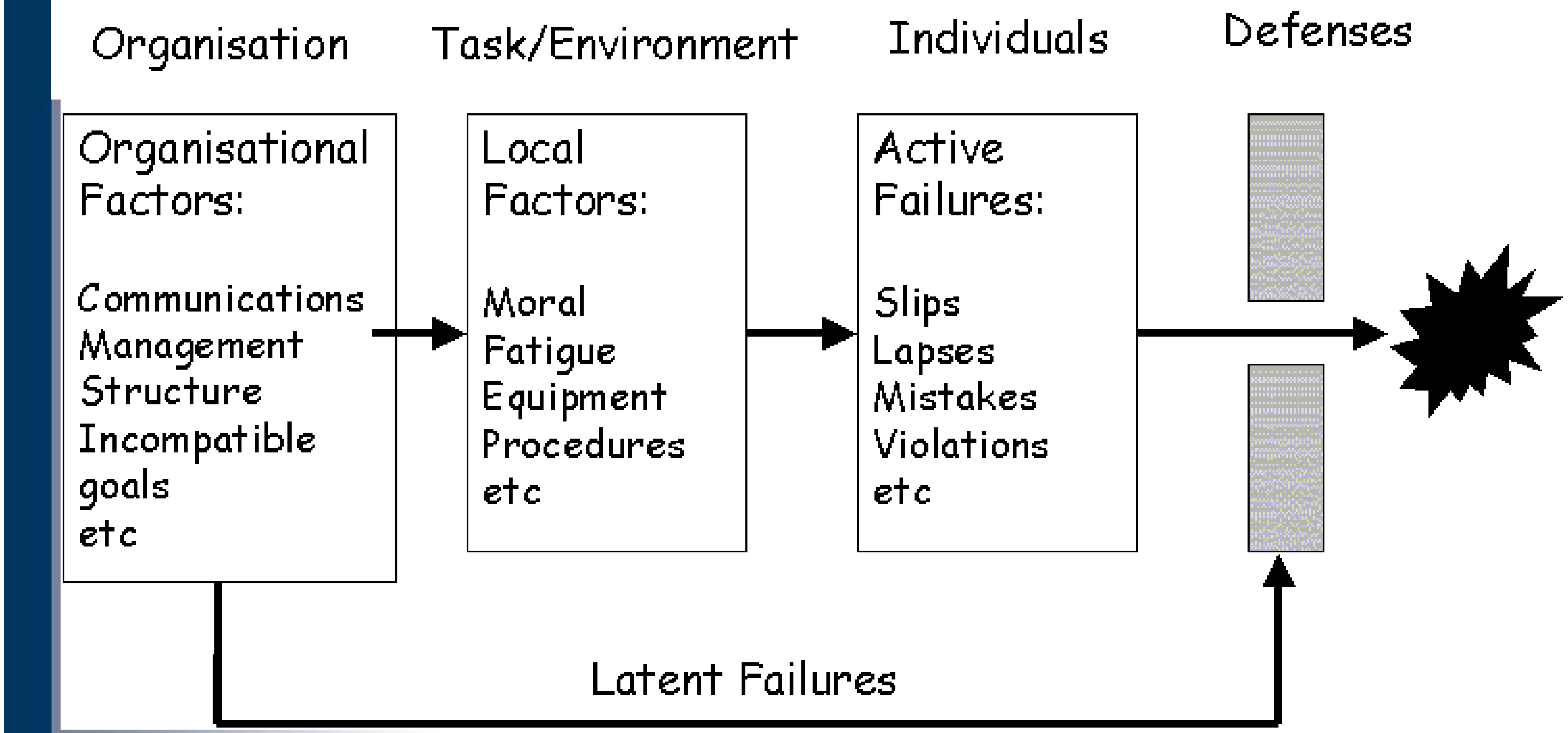
Security

Ack: J.C. Laprie

Terminology

- What is `Safety'?
- Must also consider failures of safety.
- Freedom from accidents or Losses (Leveson).
- So what is an accident?

Terminology



Organisation

Task/Environment

Individuals

Defenses

Organisational Factors:

Communications
Management
Structure
Incompatible goals
etc

Local Factors:

Moral
Fatigue
Equipment
Procedures
etc

Active Failures:

Slips
Lapses
Mistakes
Violations
etc

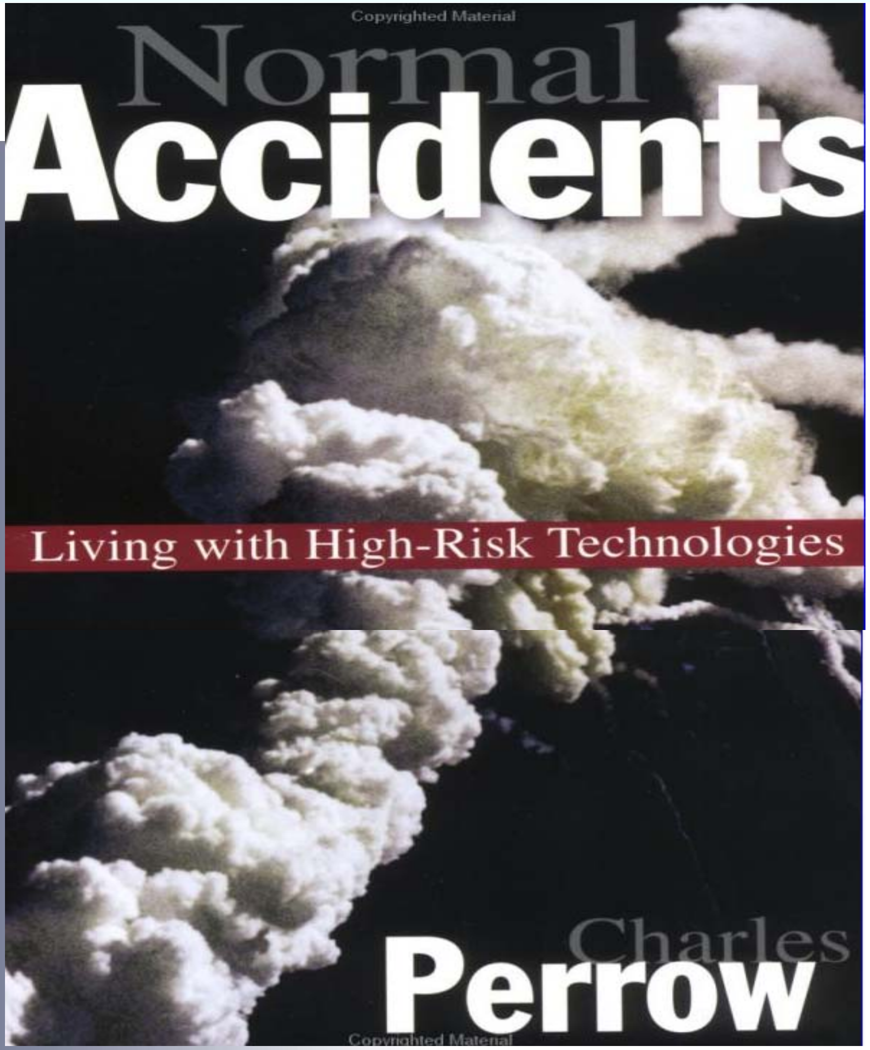
Latent Failures

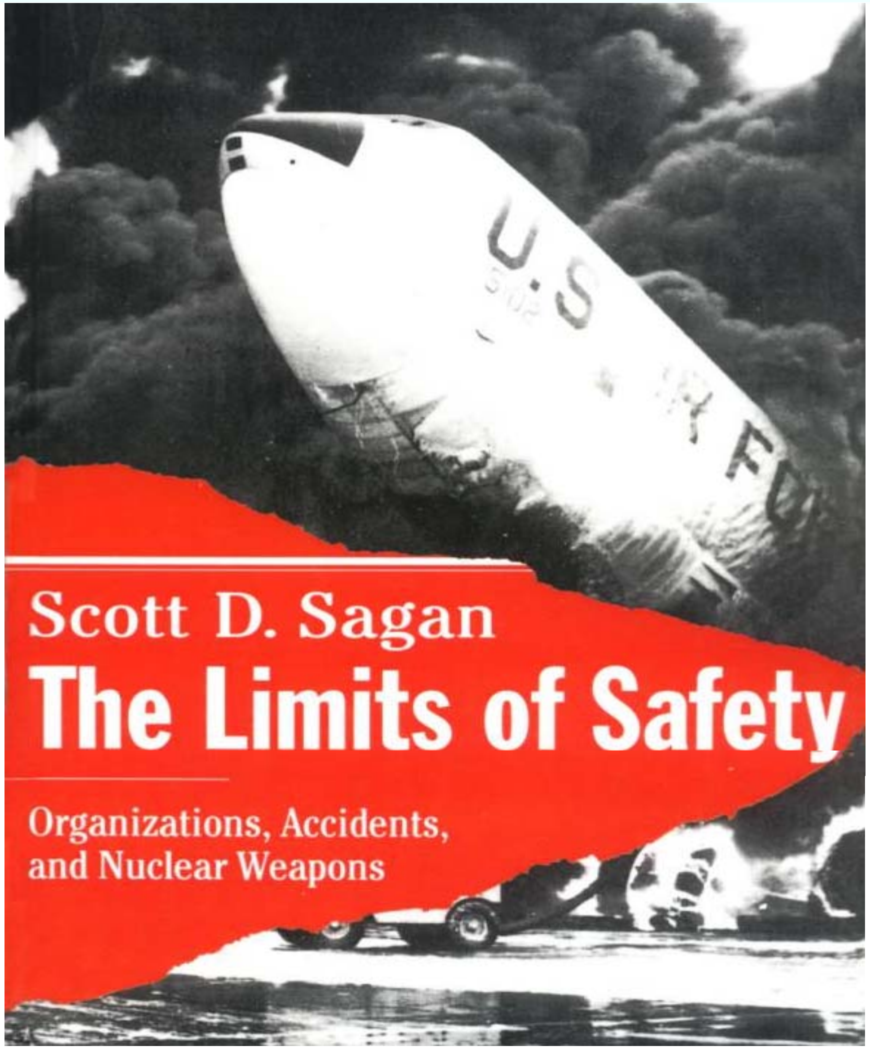
Taken from Reason, Managing the Risks of Organisational Failure, Ashgate Publishing, 1997.

Terminology

- Accidents have multiple causes.
- Some are latent.
- Triggered by catalytic events.
- We should expect failure.
- Perrows' Normal Accidents?

Normal Accidents…





Terminology

- What is `Safety'?
- Is it an emmergent property?
- SYSTEMS continually change.
- So level of safety changes.
- For instance, ABS braking?

Some Key Ideas

- As Low As Reasonably Practicable (ALARP).

“A risk is ALARP when it has been demonstrated that the cost of any further Risk Reduction, where the cost includes the loss of defence capability as well as financial or other resource costs, is grossly disproportionate to the benefit obtained from that Risk Reduction.”

(UK MOD Def Stan 00-56 Issue 4)

Some Key Ideas

- As Low As Reasonably Achievable (ALARA)
  - US military doctrine, cost less of a factor?
- Minimum Endogenous Mortality (MEM):
  - Used in Germany etc
  - do not introduce hazards that ‘significantly increase’ death rate beyond that from disease, congenital mortality etc
- All are heuristics and hard to demonstrate…

The Ariane 5 Case Study

The Ariane 5 Case Study

- Variable exceeds it's range...

e) At 36.7 seconds after H0 (approx. 30 seconds after lift-off) the computer within the back-up inertial reference system, which was working on stand-by for guidance and attitude control, became inoperative. This was caused by an internal variable related to the horizontal velocity of the launcher exceeding a limit which existed in the software of this computer.

The Ariane 5 Case Study

- Defences in depth' failed...

f) Approx. 0.05 seconds later the active inertial reference system, identical to the back-up system in hardware and software, failed for the same reason. Since the back-up inertial system was already inoperative, correct guidance and attitude information could no longer be obtained and loss of the mission was inevitable.

The Ariane 5 Case Study

- Error stemmed from redundant code!

m) The inertial reference system of Ariane 5 is essentially common to a system which is presently flying on Ariane 4. The part of the software which caused the interruption in the inertial system computers is used before launch to align the inertial reference system and, in Ariane 4, also to enable a rapid realignment of the system in case of a late hold in the countdown. This realignment function, which does not serve any purpose on Ariane 5, was nevertheless retained for commonality reasons and allowed, as in Ariane 4, to operate for approx. 40 seconds after lift-off.

The Ariane 5 Case Study

- Problems in requirements/safety analysis.

n) During design of the software of the inertial reference system used for Ariane 4 and Ariane 5, a decision was taken that it was not necessary to protect the inertial system computer from being made inoperative by an excessive value of the variable related to the horizontal velocity, a protection which was provided for several other variables of the alignment software. When taking this design decision, it was not analysed or fully understood which values this particular variable might assume when the alignment software was allowed to operate after lift-off.

The Ariane 5 Case Study

- Failed to understand system change?

o) In Ariane 4 flights using the same type of inertial reference system there has been no such failure because the trajectory during the first 40 seconds of flight is such that the particular variable related to horizontal velocity cannot reach, with an adequate operational margin, a value beyond the limit present in the software.

p) Ariane 5 has a high initial acceleration and a trajectory which leads to a build-up of horizontal velocity which is five times more rapid than for Ariane 4. The higher horizontal velocity of Ariane 5 generated, within the 40-second timeframe, the excessive value which caused the inertial system computers to cease operation

The Ariane 5 Case Study

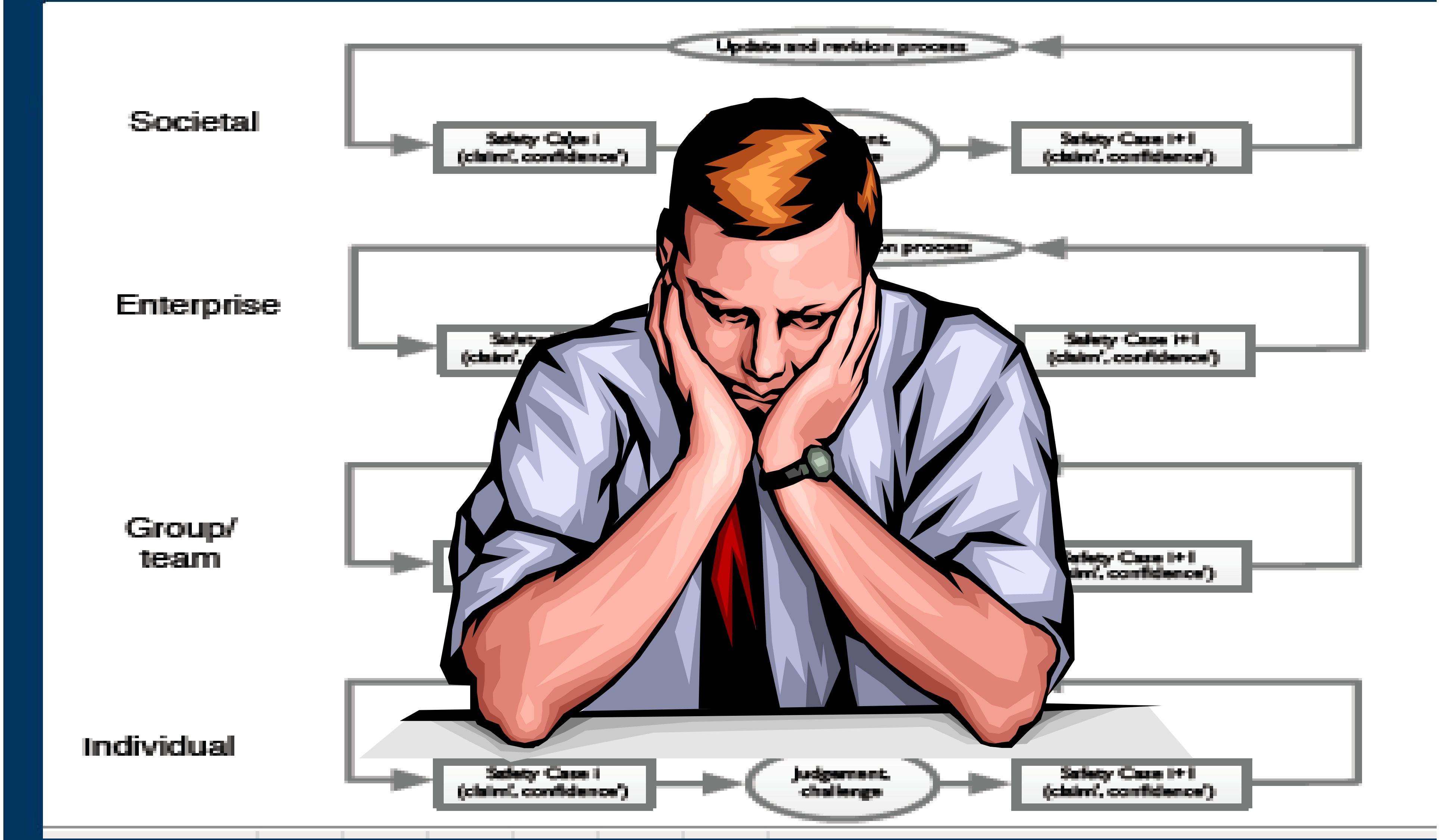
It has been stated to the Board that not all the conversions were protected because a maximum workload target of 80% had been set for the SRI computer. To determine the vulnerability of unprotected code, an analysis was performed on every operation which could give rise to an exception, including an Operand Error. In particular, the conversion of floating point values to integers was analysed and operations involving seven variables were at risk of leading to an Operand Error. This led to protection being added to four of the variables, evidence of which appears in the Ada code. However, three of the variables were left unprotected. No reference to justification of this decision was found directly in the source code. Given the large amount of documentation associated with any industrial application, the assumption, although agreed, was essentially obscured, though not deliberately, from any external review.

Section 2.2 COMMENTS ON THE FAILURE SCENARIO, paragraph 2

Conclusions

- Safety is:
  - freedom from accidents/losses.
- Accidents are:
  - complex multi-causal events;
  - (almost) impossible to predict.
- Therefore hard to maintain safety.
- This course tries to show you how...

Any Questions…


Update and revision process
Societal
Safety Case i
(claim', confidence')
Safety Case i+1
(claim', confidence')
Enterprise
process
Safety Case i+1
(claim', confidence')
Group/
team
Safety Case i+1
(claim', confidence')
Individual
Safety Case i
(claim', confidence')
Judgement,
challenge
Safety Case i+1
(claim', confidence')